Identitites for Field Extensions Generalizing the Ohno–Nakagawa Relations

Henri Cohen, Simon Rubinstein-Salzedo, Frank Thorne

IDENTITIES FOR FIELD EXTENSIONS GENERALIZING THE OHNO–NAKAGAWA RELATIONS

HENRI COHEN, SIMON RUBINSTEIN-SALZEDO, AND FRANK THORNE

Abstract. In previous work, Ohno [Ohn97] conjectured, and Nakagawa [Nak98] proved, relations between the counting functions of certain cubic fields. These relations may be viewed as complements to the Scholz reflection principle, and Ohno and Nakagawa deduced them as consequences of 'extra functional equations' involving the Shintani zeta functions associated to the prehomogeneous vector space of binary cubic forms.

In the present paper we generalize their result by proving a similar identity relating certain degree ℓ fields with Galois groups D_ℓ and F_ℓ respectively, for any odd prime ℓ, and in particular we give another proof of the Ohno–Nakagawa relation without appealing to binary cubic forms.

1. Introduction

Let $N_3(D)$ denote the number of cubic fields of discriminant D. The starting point of this paper is the following theorem of Nakagawa [Nak98], which had been previously conjectured by Ohno [Ohn97].

Theorem 1.1. [Nak98, Ohn97] *Let $D \neq 1, -3$ be a fundamental discriminant. We have*

$$N_3(D^*) + N_3(-27D) = \begin{cases} N_3(D) & \text{if } D < 0\ , \\ 3N_3(D) + 1 & \text{if } D > 0\ , \end{cases} \tag{1.1}$$

where $D^* = -3D$ if $3 \nmid D$ and $D^* = -D/3$ if $3 \mid D$.

Their result is closely related to that which can be derived from the classical reflection principle of Scholz [Sch32], which omits the terms $N_3(-27D)$ and provides for two possibilities for each term on the right. The significance of D^* is that $\mathbb{Q}(\sqrt{D^*})$ is the *mirror field* of $\mathbb{Q}(\sqrt{D})$, the quadratic subfield of $\mathbb{Q}(\sqrt{D}, \zeta_3)$ distinct from $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\zeta_3)$.

Nakagawa deduced his result from a careful study of the arithmetic of binary cubic forms, which yielded an 'extra functional equation' for the associated Shintani zeta functions. It appears that such 'extra functional equations' might be a common feature in the theory of prehomogeneous vector spaces; for example, in unpublished work Nakagawa and Ohno [NO] have conjectured a related formula for the prehomogeneous vector space $(\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$, which as Bhargava demonstrated in [Bha04, Bha05], may be used to count quartic fields. Nakagawa has made substantial headway toward proving this formula, but it appears that there are still many technical details to be overcome.

In this paper we demonstrate that the Ohno–Nakagawa results can be generalized in a different direction, in which cubic fields are replaced by certain degree ℓ-fields for any odd prime ℓ, using a framework involving class field theory and Kummer theory, and which also gives another proof of Theorem 1.1.

Date: January 8, 2015.

For an odd prime ℓ, we say that a degree ℓ number field is a *D_ℓ-field* if its Galois closure is dihedral of order 2ℓ, and an *F_ℓ-field* if its Galois closure has Galois group F_ℓ, defined by

$$F_\ell := \langle \sigma, \tau : \sigma^\ell = \tau^{\ell-1} = 1, \tau\sigma\tau^{-1} = \sigma^g \rangle \,, \tag{1.2}$$

for a primitive root $g \pmod{\ell}$. (Note that different primitive roots give isomorphic groups, but for our purposes it will be important to specify which primitive root is taken.) For $\ell = 3$ we have $D_3 = F_3 = S_3$, so this distinction is not apparent.

We observe the convention that discriminants always specify the number of pairs of complex embeddings. These will be indicated by powers of D and -1 (e.g., if D is negative, D^k indicates k pairs of complex embeddings and $(-D)^k$ indicates none). Thus $(-1)^{r_2}|D|^k$ will mean that specific discriminant, with r_2 pairs of complex embeddings (so this is different from, say, $(-1)^{r_2+2}|D|^k$). Subject to this convention, we write $N_{D_\ell}(D)$ and $N_{F_\ell}(D)$ for the number of D_ℓ- and F_ℓ-fields of discriminant D. Our main theorems, as in Theorem 1.1, will relate $N_{D_\ell}(D)$ and $N_{F_\ell}(D')$ for related values of D, D'.

For $\ell > 5$, our methods will not relate *all* F_ℓ-fields of discriminant D' to D_ℓ-fields; we require an additional Galois theoretic condition on our F_ℓ-fields which we now describe. The Galois closure E' of each F_ℓ-field E that we count will be a degree ℓ extension of a degree $\ell - 1$ field K', cyclic over $\mathbb{Q}$. (See Theorem 2.12.) In turn, each K' will be a subfield of the degree $2(\ell-1)$ extension $K_z := \mathbb{Q}(\sqrt{D}, \zeta_\ell)$ (we assume that $D \neq (-1)^{\frac{\ell-1}{2}}\ell$); we will call K' the *mirror field* of of $K = \mathbb{Q}(\sqrt{D})$.

Choose and fix a primitive root $g \pmod{\ell}$, and define τ to be the unique element of $\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ with $\tau(\zeta_\ell) = \zeta_\ell^g$. We write also τ for the unique lift of this element to $\mathrm{Gal}(K_z/K)$, and for its unique restriction to an element of $\mathrm{Gal}(K'/\mathbb{Q})$. (We will have $K \cap K' = \mathbb{Q}$.)

The group $\mathrm{Gal}(K'/\mathbb{Q})$ acts on $\mathrm{Gal}(E'/K')$ by conjugation, and we require this action to match (1.2) *for the choices of τ and g already made*. More precisely, suppose E' is such an extension of K', let τ denote any lift of the $\tau \in \mathrm{Gal}(K'/\mathbb{Q})$ from the last paragraph to $\mathrm{Gal}(E'/\mathbb{Q})$, and let $\sigma \in \mathrm{Gal}(E'/K') \leq \mathrm{Gal}(E'/\mathbb{Q})$ be any element of order ℓ. Then we require that $\tau\sigma\tau^{-1} = \sigma^g$. (This is independent of the choice of lift of τ and of σ.) We write $N^*_{F_\ell}(D)$ for the number of F_ℓ-fields of discriminant D satisfying this condition.

We will show in Lemma 2.11 that any F_ℓ field with the discriminants we count has a mirror field as its $C_{\ell-1}$ subfield. With notation as above we must have $\tau\sigma\tau^{-1} = \sigma^{g'}$ for some primitive root g' modulo ℓ, so our condition may be stated as requiring that $g' = g$. Moreover, there are many F_ℓ fields whose discriminants we do not count — for example, fields of the form $\mathbb{Q}(\sqrt[\ell]{a})$ for $a \in \mathbb{Q}^\times \setminus \mathbb{Q}^{\times\ell}$ and $\ell \geq 5$; the $C_{\ell-1}$ subfield of all these fields is $\mathbb{Q}(\zeta_\ell)$. Our work raises a variety of questions regarding the relative frequencies of the fields being counted; we expect that these questions may be quite difficult to answer, and in any case we leave them for later investigation.

This brings us to the presentation of our main results:

Theorem 1.2. *For each negative fundamental discriminant $D \neq -\ell$ we have*

$$N_{D_\ell}(D^{\frac{\ell-1}{2}}) = \begin{cases} N^*_{F_\ell}((-1)^0\ell^{\ell-2}|D|^{\frac{\ell-1}{2}}) + N^*_{F_\ell}((-1)^0\ell^\ell|D|^{\frac{\ell-1}{2}}) & \text{if } \ell \nmid D \,, \\ N^*_{F_\ell}((-1)^0\ell^{\frac{\ell-3}{2}}|D|^{\frac{\ell-1}{2}}) + N^*_{F_\ell}((-1)^0\ell^\ell|D|^{\frac{\ell-1}{2}}) & \text{if } \ell \mid D \text{ and } \ell \equiv 1 \pmod 4 \,, \\ N^*_{F_\ell}((-1)^0\ell^{\frac{\ell-5}{2}}|D|^{\frac{\ell-1}{2}}) + N^*_{F_\ell}((-1)^0\ell^\ell|D|^{\frac{\ell-1}{2}}) & \text{if } \ell \mid D \text{ and } \ell \equiv 3 \pmod 4 \,. \end{cases} \tag{1.3}$$

For positive discriminants we obtain the following close analogue, reflecting the difference between positive and negative D in the Ohno–Nakagawa relation.

Theorem 1.3. *For each positive fundamental discriminant $D \neq 1, \ell$ we have*

(1.4)
$$\ell N_{D_\ell}(D^{\frac{\ell-1}{2}})+1 = \begin{cases} N^*_{F_\ell}((-1)^{\frac{\ell-1}{2}}\ell^{\ell-2}D^{\frac{\ell-1}{2}}) + N^*_{F_\ell}((-1)^{\frac{\ell-1}{2}}\ell^{\ell}D^{\frac{\ell-1}{2}}) & \text{if } \ell \nmid D\ , \\ N^*_{F_\ell}((-1)^{\frac{\ell-1}{2}}\ell^{\frac{\ell-3}{2}}D^{\frac{\ell-1}{2}}) + N^*_{F_\ell}((-1)^{\frac{\ell-1}{2}}\ell^{\ell}D^{\frac{\ell-1}{2}}) & \text{if } \ell \mid D \text{ and } \ell \equiv 1 \pmod 4\ , \\ N^*_{F_\ell}((-1)^{\frac{\ell-1}{2}}\ell^{\frac{\ell-5}{2}}D^{\frac{\ell-1}{2}}) + N^*_{F_\ell}((-1)^{\frac{\ell-1}{2}}\ell^{\ell}D^{\frac{\ell-1}{2}}) & \text{if } \ell \mid D \text{ and } \ell \equiv 3 \pmod 4\ . \end{cases}$$

Nakagawa's Theorem 1.1 is the case $\ell = 3$ of these results.

In fact we prove something slightly stronger: The right-hand sides of (1.3) and (1.4) list two possibilities ℓ^b and $\ell^{b'}$ for the power of ℓ in the discriminants of F_ℓ-fields, but they do not rule out other powers of ℓ that may occur in F_ℓ-field discriminants with the desired Galois condition. Our proof (see Proposition 3.10) shows that in fact there are no F_ℓ-fields with the given Galois condition and exponents of ℓ between 0 and $\frac{3\ell-1}{2}$ other than the ones that appear on the right-hand sides of (1.3) and (1.4). (Larger exponents do occur, and they do not appear to correspond to D_ℓ-fields.)

A special consideration arises when $\ell \equiv 1 \pmod 4$. Suppose that $d \neq 1$ is a fundamental discriminant not divisible by ℓ. Then, D_ℓ-fields of discriminant $D^{\frac{\ell-1}{2}}$ with $D = d$ and $D = d\ell$ respectively correspond to F_ℓ-fields enumerated on the first and second lines on the right of (1.3) or (1.4). It is easily checked that the discriminants and signatures of F_ℓ-fields enumerated in the first terms on these two lines (for $D = d$ and $D = d\ell$ respectively) are identical, so that the only difference between them consists of the condition implied by the star.

It will be proved later that $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{\ell d})$ have the same mirror field when $\ell \equiv 1 \pmod 4$. However, our definition of $\tau \in \mathrm{Gal}(K'/\mathbb{Q})$ involved lifting an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ to $\mathrm{Gal}(K_z/K)$ and therefore depends on K. Writing τ' and τ'' for the elements τ determined when $K = \mathbb{Q}(\sqrt{d})$ and $K = \mathbb{Q}(\sqrt{\ell d})$ respectively, we will see later (in Remark 3.9) that the condition $\tau''\sigma\tau''^{-1} = \sigma^g$ of (1.2) is equivalent to $\tau'\sigma\tau'^{-1} = \sigma^{-g}$. (Note that for a primitive root $g \pmod \ell$ with $\ell \equiv 1 \pmod 4$, $-g$ is also a primitive root.)

When $\ell = 5$ there are only two primitive roots, so letting g be either of them we find that all F_5-fields satisfy $\tau'\sigma\tau'^{-1} = \sigma^g$ or $\tau'\sigma\tau'^{-1} = \sigma^{-g}$. Therefore, by counting D_5-fields of discriminant with $D = d$ and $D = \ell d$ together we obtain a corresponding count of F_5-fields without any Galois condition:

Corollary 1.4. *If D is a negative fundamental discriminant coprime to 5, we have*

$$N_{D_5}\big(D^2\big) + N_{D_5}\big(5D^2\big) = N_{F_5}\big((-1)^0 5^3|D|^2\big) + N_{F_5}\big((-1)^0 5^5|D|^2\big) + N_{F_5}\big((-1)^0 5^7|D|^2\big)\ . \tag{1.5}$$

and if $D \neq 1$ is a positive fundamental discriminant coprime to 5, we have

$$5\Big(N_{D_5}\big(D^2\big) + N_{D_5}\big((5D)^2\big)\Big) + 2 = N_{F_5}\big((-1)^2 5^3 D^2\big) + N_{F_5}\big((-1)^2 5^5 D^2\big) + N_{F_5}\big((-1)^2 5^7 D^2\big)\ . \tag{1.6}$$

Another (immediate) corollary of our results is that F_ℓ-fields of certain discriminants must exist.

Corollary 1.5. *For each positive fundamental discriminant D coprime to $\ell - 1$, there exists at least one F_ℓ-field with discriminant of the form $(-1)^{\frac{\ell-1}{2}}\ell^a D^{\frac{\ell-1}{2}}$, for some a as described above. If $\ell \equiv 1 \pmod 4$, there exist at least two.*

Further directions. There are multiple directions in which one might ask for extensions of our results. The most obvious is to drop the requirement that D be a fundamental discriminant. However, as was observed by Nakagawa, no simple relation appears to hold even for $\ell = 3$. Examining a table of cubic fields suggests that any result along these lines would need to account for more subtle information than simply counts of field discriminants.

Similarly, one could attempt to allow additional factors of ℓ in our counts for D_ℓ-fields. This might involve generalizations of the results of Section 3, some of which are carried out in Section 8 of [CT13b], along with further study of the sizes of various groups appearing in these results.

Motivated by Nakagawa's results, one might try to prove a result counting *ring* discriminants. In this context, Ohno and Nakagawa *did* obtain beautiful and simple relations among all discriminants, by considering (equivalently): cubic *rings* (including reducible and nonmaximal rings); binary cubic forms up to $\mathrm{SL}_2(\mathbb{Z})$-equivalence; or the Shintani zeta functions associated to this lattice of binary cubic forms.

The equivalences among these objects do not naturally generalize to $\ell > 3$, and in particular there is no naturally associated zeta function which is known (to the authors, at least) to have good analytic properties. Therefore, it seems that the Ohno–Nakagawa relations for cubic rings may be special to the prime $\ell = 3$. However, it is not out of the question that our work could be extended to an Ohno–Nakagawa relation counting appropriate subsets of the set of rings of rank ℓ. In any case work of Nakagawa [Nak96] and Kaplan, Marcinek, and Takloo-Bighash [KMTB13] (among others) suggests that enumerating such rings is likely to be quite difficult.

Remark 1.6. As F. Calegari explained to us, alternative proofs of our results can also be given in the language of cohomology and Galois representations, as a consequence of Poitou-Tate duality [Poi67, Tat63] and a formula of Greenberg [Gre89] and Wiles [Wil95] (see also Theorem 2.18 of [DDT97]).

Methods of proof and summary of the paper. The proofs involve the use of class field theory and Kummer theory, along the lines developed by the first author and a variety of collaborators (see, e.g., [CDyDO06, Coh04, CM11, CT14, CT13a, CT13b]) to enumerate fields with fixed resolvent. Especially relevant is work of the first and third authors [CT13b], giving an explicit formula for the Dirichlet series $\sum_K |\mathrm{Disc}(K)|^{-s}$, where the sum is over all D_ℓ-fields K with a *fixed* quadratic resolvent. The results of the present paper (or, for $\ell = 3$, of Nakagawa) are required to put this formula into its most explicit form, as a sum of Euler products indexed by F_ℓ-fields. Our main theorem precisely determines the indexing set of F_ℓ-fields, and yields the constant term of the main identity of [CT13b].

Our work has an earlier antecedent in the proof of the Scholz reflection principle, as presented for example in Washington's book [Was97]. Let K, K_z, and K' be as described previously. The technical heart of this paper is the Kummer pairing of Corollary 3.2, together with its consequence Proposition 3.5. Our variant of the pairing relates the ray class group $\mathrm{Cl}_{\mathfrak{b}}(K_z)/\mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell$ (for an ideal $\mathfrak{b}$ to be described) with a subgroup of $K_z^\times/(K_z^\times)^\ell$ known as an *arithmetic Selmer group*. Applying a theorem of Hecke will allow us to conclude, in contrast to the situation in [Was97], that this pairing is perfect.

It is also Galois equivariant, so we can isolate pieces of the ray class group and Selmer group which 'come from' subfields of K_z: the Selmer group comes from K (Proposition 3.4), and the ray class group comes from K' (Proposition 3.6). In Proposition 3.7 we will see directly that this ray class group counts F_ℓ-fields. On the Selmer side our argument will be less direct: computations from previous work yield Proposition 3.5, relating the size of this Selmer group to $|\mathrm{Cl}(K)/\mathrm{Cl}(K)^\ell|$. This latter class group counts the D_ℓ-fields enumerated in our main theorems, as we recall in Lemma 2.8.

In Section 2 we establish a variety of preliminary results on the arithmetic of D_ℓ and F_ℓ-extensions. The most involved result is Theorem 2.12, which guarantees that the Galois closure E' of each F_ℓ-field E we count contains K', as required for our main theorems to make sense.

In Section 3 we study the Kummer pairing as described above. We wrap up the proofs in Section 4; essentially the only part remaining is to compute the discriminants of the F_ℓ-fields being counted. Finally, in Section 5 we describe some numerical tests of our results, accompanied by a comment on the `Pari/GP` program (available from the third author's website) used to generate them.

Acknowledgments

We would like to thank Frank Calegari, Jürgen Klüners, Hendrik Lenstra, David Roberts, John Voight, and the referees for helpful discussions and suggestions related to this work.

2. Preliminaries

In this section we introduce some needed machinery and notation, and prove a variety of results about the D_ℓ- and F_ℓ-fields counted by our theorems. Throughout, ℓ is a fixed odd prime.

2.1. **Group theory.** We write C_r for the cyclic group of order r and D_r for the dihedral group of order $2r$. When $r = \ell$ is an odd prime, we write F_ℓ for the Frobenius group defined in (1.2). The Frobenius group may be realized as the group of affine transformations $x \mapsto ax + b$ over $\mathbb{F}_\ell$ with $a \in \mathbb{F}_\ell^\times$ and $b \in \mathbb{F}_\ell$. The subgroup generated by σ (equivalently, the subgroup of translations) is normal, and all nontrivial proper normal subgroups contain $\langle\sigma\rangle$.

The following results are standard and easily checked (granting the basic results of class field theory), and so we omit their proofs.

Lemma 2.1. *Suppose that $K \subset K' \subset K''$ is a tower of field extensions, with K'/K, K''/K', and K''/K all Galois, and write τ and σ for elements of $\mathrm{Gal}(K'/K)$ and $\mathrm{Gal}(K''/K')$ respectively. Then:*

1. *$\mathrm{Gal}(K'/K)$ acts on $\mathrm{Gal}(K''/K')$ by conjugation; for $\tau \in \mathrm{Gal}(K'/K), \sigma \in \mathrm{Gal}(K''/K')$, the action is defined by $\tau\sigma\tau^{-1} := \widetilde{\tau}\sigma\widetilde{\tau}^{-1}$ for an arbitrary lift $\widetilde{\tau}$ of τ to $\mathrm{Gal}(K''/K)$.*
2. *If further K'' corresponds via class field theory to an ℓ-torsion quotient $\mathrm{Cl}_{\mathfrak{a}}(K')/B$ of a ray class group of K', on which $\tau \in \mathrm{Gal}(K'/K)$ acts by $\tau(x) = x^a$ for some $a \in \mathbb{F}_\ell^\times$, then the conjugation action of $\mathrm{Gal}(K'/K)$ on $\mathrm{Gal}(K''/K')$ is given by $\tau\sigma\tau^{-1} = \sigma^a$.*

2.2. **Background on conductors.** We recall some basic facts about conductors of extensions of local and global fields, following [Ser67].

Definition 2.2. Let L/K be a finite abelian extension of local fields. Let $\mathfrak{p}$ be the maximal ideal of $\mathbb{Z}_K$. We define the *local conductor* $\mathfrak{f}(L/K)$ to be the least integer n so that

$$1 + \mathfrak{p}^n \subseteq N_{L/K}(L^\times) .$$

The local conductor thus gives us information about the ramification type of L/K. In particular:

Proposition 2.3. 1. *L/K is unramified if $\mathfrak{f}(L/K) = 0$, tamely ramified if $\mathfrak{f}(L/K) = 1$, and wildly ramified if $\mathfrak{f}(L/K) > 1$.*
2. *If $M/L/K$ is a tower of extensions of local fields with M/K abelian and L/K unramified, then $\mathfrak{f}(M/K) = \mathfrak{f}(M/L)$.*

If $K = \mathbb{Q}_p$, we will sometimes write $\mathfrak{f}(L)$ rather than $\mathfrak{f}(L/\mathbb{Q}_p)$. Also, if L/K is an abelian extension of *global* fields, $\mathfrak{p}$ a prime of K and $\mathfrak{P}$ a prime of L above $\mathfrak{p}$, we will sometimes write $\mathfrak{f}_\mathfrak{p}(L/K)$ for $\mathfrak{f}(L_\mathfrak{P}/K_\mathfrak{p})$, since this does not depend on $\mathfrak{P}$. Here, $L_\mathfrak{P}$ and $K_\mathfrak{p}$ denote the $\mathfrak{P}$-adic and $\mathfrak{p}$-adic completions of L and K, respectively.

Definition 2.4. Let L/K be a finite abelian extension of global fields, set

$$\mathfrak{f}_0(L/K) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathfrak{f}_{\mathfrak{p}}(L/K)} ,$$

and let $\mathfrak{f}_\infty(L/K)$ denote the set of real places of K ramified in L. The *global conductor* of L/K is defined to be the modulus $\mathfrak{f}(L/K) = \mathfrak{f}_0(L/K)\mathfrak{f}_\infty(L/K)$.

Proposition 2.5. *If $L/\mathbb{Q}$ is a finite abelian extension, then $\mathfrak{f}_0(L/\mathbb{Q})$ is the ideal of $\mathbb{Z}$ generated by the least number n so that $L \subseteq \mathbb{Q}(\zeta_n)$.*

Proposition 2.6. *If L/K be a quadratic extension of global fields, then $\mathfrak{f}_0(L/K) = \mathrm{Disc}(L/K)$.*

2.3. **The field diagram.** We fix a primitive ℓ^{th} root of unity ζ_ℓ and a primitive root $g \pmod{\ell}$. Let $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell$, so that $\mathbb{Q}(\sqrt{\ell^*})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_\ell)$.

Let D be a fundamental discriminant, and let $K = \mathbb{Q}(\sqrt{D})$, where we assume that $D \neq \ell^*$ (although we could presumably handle this case as well).

Write $K_z = K(\zeta_\ell)$, with $[K_z : \mathbb{Q}] = 2(\ell-1)$ and $\Gamma = \mathrm{Gal}(K_z/\mathbb{Q}) \cong C_2 \times (\mathbb{Z}/\ell\mathbb{Z})^\times$. By Kummer theory, degree ℓ abelian extensions of K_z are all of the form $K_z(\alpha^{1/\ell})$ for some $\alpha \in K_z$. Write τ and τ_2 for the elements of Γ fixing K and $\mathbb{Q}(\zeta_\ell)$ respectively, with $\tau(\zeta_\ell) = \zeta_\ell^g$, and τ_2 nontrivial on K. We also write

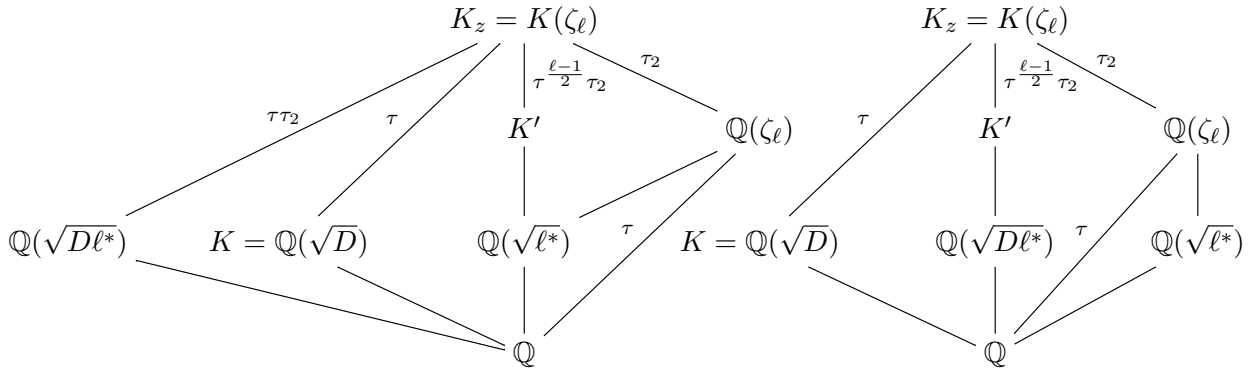
$$T = \{\tau - g, \tau_2 + 1\},\ T^* = \{\tau - 1, \tau_2 + 1\} \subseteq \mathbb{F}_\ell[\Gamma] . \tag{2.1}$$

The *mirror field K' of K* is the fixed field of $\tau_2\tau^{\frac{\ell-1}{2}}$; more explicitly,

$$K' = \mathbb{Q}\big((\zeta_\ell - \zeta_\ell^{-1})\sqrt{D}\big) = \mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})\Big(\sqrt{-D\big(4 - (\zeta_\ell + \zeta_\ell^{-1})^2\big)}\Big) . \tag{2.2}$$

In particular, K' is a quadratic extension of the maximal totally real subfield of $\mathbb{Q}(\zeta_\ell)$, it is cyclic of degree $\ell - 1$ over $\mathbb{Q}$, with Galois group generated by the restriction of τ to K', and its unique quadratic subfield is equal to $\mathbb{Q}(\sqrt{\ell^*})$ if $\ell \equiv 1 \pmod 4$ and to $\mathbb{Q}(\sqrt{D\ell^*})$ if $\ell \equiv 3 \pmod 4$.

We thus have the following diagrams of fields in the $\ell \equiv 1 \pmod 4$ and $\ell \equiv 3 \pmod 4$ cases respectively.



The mirror field of $\mathbb{Q}(\sqrt{D\ell^*})$ is fixed by $(\tau\tau_2)^{\frac{\ell-1}{2}}\tau_2$, which is equal to $\tau^{\frac{\ell-1}{2}}\tau_2$ if $\ell \equiv 1 \pmod 4$ and to $\tau^{\frac{\ell-1}{2}}$ if $\ell \equiv 3 \pmod 4$. Hence if $\ell \equiv 1 \pmod 4$ then the fields K and $\mathbb{Q}(\sqrt{D\ell^*})$ share the same mirror field, and if $\ell \equiv 3 \pmod 4$ they do not. If $\ell = 3$ then $K' = \mathbb{Q}(\sqrt{D\ell^*})$ and $\mathbb{Q}(\zeta_\ell) = \mathbb{Q}(\sqrt{\ell^*})$, so the second row of the diagram should be identified with the third.

Notation for splitting types. We write (as is fairly common) that a prime $\mathfrak{p}$ of a field K has splitting type $(f_1^{e_1} f_2^{e_2} \dots f_g^{e_g})$ in L/K if $\mathfrak{p}\mathbb{Z}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$ with $f(\mathfrak{P}_i|\mathfrak{p}) = f_i$ for each i.

2.4. **Selmer groups of number fields.** In Section 3 our results will be phrased in terms of the ℓ-Selmer group, which measures the failure of the local-global principle for local ℓ^{th} powers to be global ℓ^{th} powers. We recall the relevant terminology here; see also [Coh00], §5.2.2.

Definition 2.7. Let L be a number field. The *group of ℓ-virtual units* $V_\ell(L)$ consists of all $u \in L^\times$ for which $u\mathbb{Z}_L = \mathfrak{a}^\ell$ for some fractional ideal $\mathfrak{a}$ of L, or equivalently all $u \in L^\times$ for which $v_\mathfrak{p}(u)$ is divisible by ℓ for all primes $\mathfrak{p}$ of L. The *ℓ-Selmer group* is the quotient $S_\ell(L) = V_\ell(L)/L^{\times\ell}$.

If $L = K_z$ then the ℓ-Selmer group is a finite ℓ-group, and it fits into a split exact sequence

$$1 \to \frac{U(K_z)}{U(K_z)^\ell} \to S_\ell(K_z) \to \mathrm{Cl}(K_z)[\ell] \to 1 \tag{2.3}$$

of $\mathbb{F}_\ell[\Gamma]$-modules.

In addition we write $\mathfrak{b} = (1-\zeta_\ell)^\ell\mathbb{Z}_{K_z}$, and for each Γ-invariant ideal $\mathfrak{c}$ of $\mathbb{Z}_{K_z}$ dividing $\mathfrak{b}$ we write

$$R_\mathfrak{c} = \mathrm{Cl}_\mathfrak{c}(K_z)/\mathrm{Cl}_\mathfrak{c}(K_z)^\ell,\ G_\mathfrak{c} = R_\mathfrak{c}[T]\ , \tag{2.4}$$

where T has been defined above. (For any $\mathbb{F}_\ell[\Gamma]$-module M, $M[T]$ denotes the subgroup annihilated by all the elements of T.) Because ℓ is totally ramified in K_z, any such $\mathfrak{c}$ must be of the form $(1-\zeta_\ell)^a\mathbb{Z}_{K_z}$ for some integer $a \le \ell$.

2.5. **The arithmetic of D_ℓ-extensions.** Our main theorems relate counts of D_ℓ- and F_ℓ-extensions of given discriminant. These fields will be constructed as subfields of their Galois closures, and our next results (and Proposition 3.7) establish the connection between these two ways of counting fields.

Lemma 2.8. *Let D be a fundamental discriminant. Then the set of D_ℓ-fields of discriminant $D^{\frac{\ell-1}{2}}$ is equal to the set of degree ℓ subfields of unramified cyclic degree ℓ extensions $L/\mathbb{Q}(\sqrt{D})$, and each prime dividing ℓ has splitting type $(1^2 1^2 \cdots 1^2 1)$ in each such D_ℓ-field.*

In particular, if $k = \mathbb{Q}(\sqrt{D})$, then up to isomorphism there are $\frac{1}{\ell-1}|\mathrm{Cl}(k)/\mathrm{Cl}(k)^\ell|$ of them.

Recall that our convention of writing discriminants in the form $\mathrm{Disc}(F) = (-1)^{r_2(F)}|\mathrm{Disc}(F)|$ specifies the number of complex embeddings of each such field.

Proof. This can be extracted from Theorem 9.2.6, Proposition 10.1.26, and Theorem 10.1.28 of [Coh00]. ∎

Remark 2.9. Our lemma does not count D_ℓ-fields of discriminant $(4D)^{\frac{\ell-1}{2}}$ arising from degree ℓ extensions of $\mathbb{Q}(\sqrt{D})$ which are ramified at 2. An example of such a field is the field generated by a root of $x^3 - x^2 - 3x + 5$ of (non-fundamental) discriminant $-2^2 67$.

Related considerations also occur on the F_ℓ side; for example, the F_5-field generated by a root of $x^5 - 2x^4 + 4x^3 + 12x^2 - 24x + 10$, of discriminant $(-1)^2 2^4 5^3 53^2$, in which 2 is totally ramified, is a non-example of a field counted by our results.

2.6. **The arithmetic of F_ℓ-extensions.** We now study the arithmetic of F_ℓ-extensions as well as the mirror fields K'. The section concludes with Theorem 2.12, which states that if E is an F_ℓ-field of appropriate discriminant then its Galois closure must contain K'.

Lemma 2.10. *Let $D \neq 1, \pm\ell$ be a fundamental discriminant, and let K' be the mirror field of $K := \mathbb{Q}(\sqrt{D})$. Then we have*

$$e_\ell(K'/\mathbb{Q}) = \begin{cases} \ell - 1 & \text{if } \ell \nmid D \text{ or } \ell \equiv 1 \pmod 4, \\ (\ell-1)/2 & \text{if } \ell \mid D \text{ and } \ell \equiv 3 \pmod 4, \end{cases}$$

$$\mathrm{Disc}(K') = \begin{cases} \ell^{\ell-2}(-D)^{(\ell-1)/2} & \text{when } \ell \nmid D, \\ \ell^{\ell-2}(-D/\ell)^{(\ell-1)/2} & \text{when } \ell \mid D \text{ and } \ell \equiv 1 \pmod 4, \\ \ell^{\ell-3}(-D/\ell)^{(\ell-1)/2} & \text{when } \ell \mid D \text{ and } \ell \equiv 3 \pmod 4, \end{cases}$$

and $e_p(K'/\mathbb{Q}) = 2$ for each prime $p \neq \ell$ dividing D.

Proof. Any prime $p \neq \ell$ dividing D is unramified in both K_z/K and K_z/K', so the formula for $v_p(\mathrm{Disc}(K'))$ follows by transitivity of the discriminant.

If $\ell \nmid D$, primes above ℓ are totally ramified in $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}$, hence in K_z/K, hence *not* in K_z/K', hence in $K'/\mathbb{Q}$. If $\ell \mid D$ and $\ell \equiv 1 \pmod 4$, this argument with K replaced by $\mathbb{Q}(\sqrt{\ell^* D})$ yields the same result. Finally, if $\ell \mid D$ and $\ell \equiv 3 \pmod 4$, then $\mathbb{Q}(\sqrt{D\ell^*})$ is unramified at ℓ and is a subextension of K', so $e_\ell(K'/\mathbb{Q}) = (\ell-1)/2$. In each of these cases, $v_\ell(\mathrm{Disc}(K'))$ is uniquely determined by (2.5) below.

The power of -1 in $\mathrm{Disc}(K')$ follows from the formula $K' = \mathbb{Q}((\zeta_\ell - \zeta_\ell^{-1})\sqrt{D})$; since K' is Galois, it is either totally real or totally complex. ∎

Lemma 2.11. *Suppose that $F/\mathbb{Q}$ is a $C_{\ell-1}$-field, with $|\mathrm{Disc}(F)|$ equal to $|D|^{\frac{\ell-1}{2}}$ times some (positive or negative) power of ℓ for a fundamental discriminant D. Then F is equal to the mirror field of $\mathbb{Q}(\sqrt{D})$ or $\mathbb{Q}(\sqrt{\ell^* D})$, with discriminant given by Lemma 2.10.*

In other words, if F has the same discriminant and signature as a mirror field K', then $F \cong K'$. If local exceptions are allowed at ℓ and infinity, then F must be one of the fields K' enumerated in Lemma 2.10, and knowing the discriminant and signature suffices to determine which.

Proof. First of all, we claim that $e_p(F/\mathbb{Q})$ is uniquely determined by $\mathrm{Disc}(F)$ for each prime p. If $p \neq 2$, then p is not wildly ramified in F, and $e_p(F/\mathbb{Q})$ may be determined from the formula

$$v_p(\mathrm{Disc}(F)) = (\ell-1)\Big(1 - \frac{1}{e_p(F/\mathbb{Q})}\Big). \tag{2.5}$$

If $p = 2$ is ramified in F, then $v_2(\mathrm{Disc}(F))$ equals either $\ell - 1$ or $3(\ell-1)/2$ and the ramification is wild. There is a unique intermediate field $\mathbb{Q} \subseteq F' \subseteq F$ with $[F : F'] = 2$ containing the inertia field. We claim that $v_2(\mathrm{Disc}(F')) = 0$: if not, by transitivity of the discriminant $v_2(\mathrm{Disc}(F')) = (\ell-1)/4$, which would imply that 2 is ramified in F' with $e_2(F'/\mathbb{Q}) = 2$ by the analogue of (2.5), which is absurd as $2 \mid [F' : \mathbb{Q}]$. Therefore $v_2(\mathrm{Disc}(F')) = 0$ and $e_2(F/\mathbb{Q}) = 2$.

We also note that each other prime $p \notin \{2, \ell\}$ which ramifies in F satisfies $e_p(F/\mathbb{Q}) = 2$ and p is unramified in F'.

The inertia groups generate $\mathrm{Gal}(F/\mathbb{Q})$ because they generate a subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ whose fixed field is everywhere unramified. If $\ell \equiv 1 \pmod 4$ the inertia group at ℓ must therefore be all of $C_{\ell-1}$. If $\ell \equiv 3 \pmod 4$ the inertia group could be the full Galois group or its index 2 subgroup, and these two cases may be distinguished by $v_\ell(\mathrm{Disc}(F))$.

Write $D_1 = \ell|D|$ if $\ell \nmid D$ and $D_1 = |D|$ if $\ell \mid D$. By Proposition 2.5 we have $F \subseteq \mathbb{Q}(\zeta_{D_1})$, as we see by computing local conductors: each prime $p \neq \ell$ is unramified in F', so that by Propositions 2.3 and 2.6 and transitivity of the discriminant we have $\mathfrak{f}_p(F) = v_{\mathfrak{p}}(\mathrm{Disc}(F_{\mathfrak{P}}/F'_{\mathfrak{p}})) = v_p(D)$, where $\mathfrak{p}$ and $\mathfrak{P}$ are primes of F' and F above p and $\mathfrak{p}$ respectively. Moreover, the prime ℓ is tamely ramified in F so that $\mathfrak{f}_\ell(F) = 1$ by Proposition 2.3.

Write $\mathrm{Gal}(\mathbb{Q}(\zeta_{D_1})/\mathbb{Q})$ as $\prod_{p^{a_p}||D_1}(\mathbb{Z}/p^{a_p})^\times$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_{D_1})/F) = A \subset \mathrm{Gal}(\mathbb{Q}(\zeta_{D_1})/\mathbb{Q})$. For each p, $A \cap (\mathbb{Z}/p^{a_p})^\times$ is the inertia group of primes above p in $\mathbb{Q}(\zeta_{D_1}/F)$, so that multiplicativity of ramification degrees implies that $[(\mathbb{Z}/p^{a_p})^\times : A \cap (\mathbb{Z}/p^{a_p})^\times] = e_p(F/\mathbb{Q})$.

Write $B_p := (\mathbb{Z}/p^{a_p})^\times$ and $B'_p := A \cap B_p$ for each p. For $p \notin \{2, \ell\}$ B'_p is the unique index 2 subgroup of B_p, and B'_ℓ is either trivial or the unique order 2 subgroup of B_ℓ, as determined above by $v_\ell(\mathrm{Disc}(F))$. B'_2 is of index 2 in B_2; if $4 \mid\mid D$, then B'_2 is uniquely determined, and if $8 \mid\mid D$ there are two possibilities for B'_2. We claim that this information uniquely determines A, except in the $8 \mid\mid D$ case where both possibilities can occur. Since the mirror fields of Lemma 2.10 satisfy all the same properties, this claim establishes the lemma.

The claim is easily checked: There is a unique subgroup $B \subseteq \prod_{p\neq\ell} B_p$ of index 2 containing $\prod_{p\neq\ell} B'_p$; it consists of vectors $(b_p)_{p\neq\ell}$ for which $b_p \notin B'_p$ for an even number of p. Moreover, B_ℓ contains a unique element b_ℓ of order 2. If $e_\ell = \ell - 1$, then A must consist of $\{1\} \times B$ and $\{b_\ell\} \times \left(\prod_{p\neq\ell} B_p - B\right)$. If $e_\ell = \frac{\ell-1}{2}$, then $A = \{1, b_\ell\} \times B$; to see that no other ℓ-component is possible, we use the fact that $\ell \equiv 3 \pmod 4$ to see that B_ℓ contains no elements of order 4. ∎

At this point we highlight the *Brauer relation* (see [FT93, Theorems 73 and 75]): If $E/\mathbb{Q}$ is a degree ℓ extension with Galois closure E' with $\mathrm{Gal}(E'/\mathbb{Q}) \cong F_\ell$, and F is the $C_{\ell-1}$ subextension of E', then

$$\zeta(s)^{\ell-1}\zeta_{E'}(s) = \zeta_E(s)^{\ell-1}\zeta_F(s)\ , \tag{2.6}$$

which implies that

$$\mathrm{Disc}(E') = \mathrm{Disc}(E)^{\ell-1}\mathrm{Disc}(F)\ . \tag{2.7}$$

(This relation also holds true for the infinite place.) This follows from a computation involving the characters of F_ℓ.

This relation also implies that $\mathrm{Disc}(E) = \mathrm{Disc}(F)\mathcal{N}(\mathfrak{f}(E'/F))$, where $\mathfrak{f}(E'/F)$ is the conductor of the abelian extension E'/F.

We can now conclude that, given suitable conditions on $\mathrm{Disc}(E)$, F must be a mirror field. Later we will apply this to count these F_ℓ-fields using class field theory.

Theorem 2.12. *Suppose that $E/\mathbb{Q}$ is an F_ℓ-field with $\mathrm{Disc}(E)$ equal to $(-D)^{\frac{\ell-1}{2}}$ times an arbitrary power of ℓ for a fundamental discriminant D. Let E' be the Galois closure of E, and let $F/\mathbb{Q}$ be the unique subextension of degree $\ell - 1$.*

Then E'/F is unramified away from the primes dividing ℓ, and F is equal to the mirror field K' of $\mathbb{Q}(\sqrt{D})$.

Proof. For the first claim, it suffices to prove that no prime $p \neq \ell$ can totally ramify in $E/\mathbb{Q}$. This is immediate for primes $p \notin \{2, \ell\}$, as $v_p(E) < \ell - 1$. However, the case $p = 2$ is more subtle: Remark 2.9 illustrates that it cannot be treated by purely local considerations.

So suppose to the contrary that 2 is totally ramified in E, so that $4 \mid\mid D$. We first claim that 2 is unramified in E/E' and therefore (because ℓ and $\ell - 1$ are coprime) also in $F/\mathbb{Q}$. To see this, we work locally. Any totally and tamely ramified extension of $\mathbb{Q}_2$ is of the form $\mathbb{Q}_2(\alpha)$, where α

is a root of $x^e - \pi$, where π is a uniformizer of $\mathbb{Q}_2$. (See [Lan94], Proposition 12 in II, §5.) Such extensions do not ramify further when we pass to the Galois closure.

For every other prime $p \neq 2, \ell$ dividing D, primes above p are unramified in E'/F, so that (2.6) and (2.5) imply that $e_p(F/\mathbb{Q}) = 2$.

Therefore, $|\mathrm{Disc}(F)|$ equals $(|D|/4)^{\frac{\ell-1}{2}}$ times a power of ℓ, so that $\mathrm{Disc}(F)$ is determined by Lemma 2.11. In particular, since $-D/4$ is a fundamental discriminant and $D/4$ is not, F is totally real if $-(-D/4) = D/4$ is positive, and totally imaginary if D is negative. However, the condition for $\mathrm{Disc}(E)$ implies that E', and therefore F, is totally real if and only if $-D$ is positive. We therefore have a contradiction.

Now we conclude from (2.7) that $\mathrm{Disc}(E) = \ell^c \mathrm{Disc}(F)$ for some $c \geq 0$, so that F satisfies the conditions of Lemma 2.11. This implies the second claim; when $\ell \equiv 3 \pmod 4$, the possibility that K' is the mirror field of $\mathbb{Q}(\sqrt{\ell^* D})$ is ruled out because the signature of E determines that of F. ■

3. The Kummer pairing and F_ℓ-fields

In this section we introduce the Kummer pairing and use it to obtain two different expressions for the size of the group $G_{\mathfrak{b}}$ (introduced at the end of Section 2.4), each of which corresponds to one of the field counts in the main theorems. Ideas for this section were contributed by Hendrik Lenstra, and we thank him for his help.

We begin with the following consequence of a classical result of Hecke.

Proposition 3.1. *Suppose that $N_z = K_z(\sqrt[\ell]{\alpha})$. Then we have $\mathfrak{f}(N_z/K_z) \mid \mathfrak{b}$ if and only if α is an ℓ-virtual unit.*

Proof. See Theorem 10.2.9 of [Coh00]. ■

Corollary 3.2. *Let $\boldsymbol{\mu}_\ell$ denote the group of ℓ^{th} roots of unity. There exists a perfect, Γ-equivariant pairing of $\mathbb{F}_\ell[\Gamma]$-modules*

$$R_{\mathfrak{b}} \times S_\ell(K_z) \to \boldsymbol{\mu}_\ell \ .$$

Proof. This is simply the Kummer pairing: let M/K_z be the abelian ℓ-extension corresponding by class field theory to $R_{\mathfrak{b}}$, which is the compositum of all cyclic degree ℓ extensions of K_z with conductors dividing $\mathfrak{b}$. If $\overline{\mathfrak{a}} \in R_{\mathfrak{b}}$, we denote as usual by $\sigma_{\mathfrak{a}} \in \mathrm{Gal}(M/K_z)$ the image of $\mathfrak{a}$ under the Artin map. Thus, by the above proposition, if $\overline{\alpha} \in S_\ell(K_z)$ and α is virtual unit representing $\overline{\alpha}$, we have $K_z(\sqrt[\ell]{\alpha}) \subset M$, and we define the pairing by

$$(\overline{\mathfrak{a}}, \overline{\alpha}) \mapsto \sigma_{\mathfrak{a}}(\sqrt[\ell]{\alpha})/\sqrt[\ell]{\alpha} \in \boldsymbol{\mu}_\ell \ ,$$

which does not depend on any choice of representatives. It is classical and immediate that this pairing is perfect and Γ-equivariant, e.g., that $\langle \tau_1(\overline{\mathfrak{a}}), \tau_1(\overline{\alpha})\rangle = \tau_1(\langle \overline{\mathfrak{a}}, \overline{\alpha}\rangle)$ for any $\tau_1 \in \Gamma$. ■

Corollary 3.3. *We have a perfect pairing*

$$G_{\mathfrak{b}} \times S_\ell(K_z)[T^*] \to \boldsymbol{\mu}_\ell \ .$$

In particular, we have

$$|G_{\mathfrak{b}}| = |S_\ell(K_z)[T^*]| \ .$$

Proof. Applying the Γ-equivariance of the pairing of the preceding corollary, and recalling that $\tau(\zeta_\ell) = \zeta_\ell^g$, for any j we obtain a perfect pairing

$$R_{\mathfrak{b}}[\tau - g^j] \times S_\ell(K_z)[\tau - g^{1-j}] \to \boldsymbol{\mu}_\ell \ .$$

Taking $j = 1$ yields a perfect pairing between $R_{\mathfrak{b}}[\tau - g]$ and $S_\ell(K_z)[\tau - 1]$, and similarly, since τ_2 leaves ζ_ℓ fixed, we obtain a perfect pairing between $G_{\mathfrak{b}} = R_{\mathfrak{b}}[\tau - g, \tau_2 + 1]$ and $S_\ell(K_z)[\tau - 1, \tau_2 + 1]$. ■

Proposition 3.4. *We have* $S_\ell(K_z)[T^*] \simeq S_\ell(K)$.

Proof. We have an evident injection

$$S_\ell(K) \longhookrightarrow S_\ell(K_z)[\tau - 1] \ ,$$

which is also surjective: if $\alpha \in K_z$ satisfies $\tau(\alpha)/\alpha = \gamma^\ell$ for some $\gamma, x \in K_z$, then $\mathcal{N}_{K_z/K}(\gamma)^\ell = \mathcal{N}_{K_z/K}(\gamma) = 1$ (since $\zeta_\ell \notin K$). By Hilbert 90 applied to K_z/K there exists $\beta \in K_z$ with $\gamma = \beta/\tau(\beta)$, hence $\tau(\alpha\beta^\ell)/(\alpha\beta^\ell) = 1$, so $a = \alpha\beta^\ell$ is a virtual unit of K_z, and also of K because $([K_z : K], \ell) = 1$.

Therefore $S_\ell(K_z)[T^*] = S_\ell(K_z)[\tau - 1, \tau_2 + 1] \simeq S_\ell(K)[\tau_2 + 1]$. On the other hand we have trivially

$$S_\ell(K) = S_\ell(K)[\tau_2 + 1] \oplus S_\ell(K)[\tau_2 - 1] \ ,$$

and we claim that $S_\ell(K)[\tau_2 - 1]$ is trivial: if $\alpha \in K$ satisfies $\tau_2(\alpha) = \alpha\gamma^\ell$ for some $\gamma \in K$, then applying τ_2 again we deduce that $(\gamma\tau_2(\gamma))^\ell = 1$ and thus $\gamma\tau_2(\gamma) = 1$, so that by a trivial case of Hilbert 90, $\gamma = \tau_2(\beta)/\beta$ for some $\beta \in K$, hence $\tau_2(\alpha/\beta^\ell) = \alpha/\beta^\ell$. Thus α/β^ℓ is a virtual unit of $\mathbb{Q}$ equivalent to α, and since $S_\ell(\mathbb{Q})$ is trivial this proves our claim and hence the proposition. ∎

We therefore have the equality $|G_{\mathfrak{b}}| = |S_\ell(K)|$, which we use to obtain the following:

Proposition 3.5. *We have*

$$|G_{\mathfrak{b}}| = \begin{cases} |\mathrm{Cl}(K)/\mathrm{Cl}(K)^\ell| & \text{if } D < 0 \ , \\ \ell|\mathrm{Cl}(K)/\mathrm{Cl}(K)^\ell| & \text{if } D > 0 \ . \end{cases} \tag{3.1}$$

Proof. By the exact sequence (2.3) and Proposition 2.12 of [CDyDO02], the proofs of which adapt to K without change, and since $\dim_{\mathbb{F}_\ell}(U(K)/U(K)^\ell) = 1 - r_2(D)$, where (as usual) $r_2 = 1$ if $D < 0$ and $r_2 = 0$ if $D > 0$, we obtain

$$|S_\ell(K)| = \ell^{1-r_2(D)}|\mathrm{Cl}(K)/\mathrm{Cl}(K)^\ell| \ ,$$

yielding the proposition. ∎

Note that the last statement generalizes Proposition 7.7 of [CM11].

By Lemma 2.8 it thus follows that D_ℓ-fields can be counted in terms of $G_{\mathfrak{b}}$. We now show that the same is true of F_ℓ-fields. We begin by showing that $G_{\mathfrak{b}}$ can be 'descended' to K', generalizing Proposition 3.4 of [CT14]:

Proposition 3.6. *Let* $\mathfrak{c} = (1 - \zeta_\ell)^a\mathbb{Z}_{K_z}$ *be any* Γ*-invariant ideal dividing* $\mathfrak{b}$.

(1) There is an isomorphism

$$\frac{\mathrm{Cl}_{\mathfrak{c}}(K_z)}{\mathrm{Cl}_{\mathfrak{c}}(K_z)^\ell}[T] \to \frac{\mathrm{Cl}_{\mathfrak{c}'}(K')}{\mathrm{Cl}_{\mathfrak{c}'}(K')^\ell}[\tau - g] \ ,$$

where K' *is the mirror field of* $K = \mathbb{Q}(\sqrt{D})$ *and* $\mathfrak{c}' = \mathfrak{c} \cap K'$.

(2) We have

- *(a)* $\mathfrak{c}' = \mathfrak{p}^a$ *if either* ℓ *is unramified in* K *or* $\ell \equiv 1 \pmod 4$, *where* $\mathfrak{p}$ *is the unique prime of* K' *above* ℓ;
- *(b)* $\mathfrak{c}' = \mathfrak{p}^{\lceil \frac{a}{2} \rceil}$ *if* ℓ *is ramified in* K *and* $\ell \equiv 3 \pmod 4$, *where* $\mathfrak{q} = \mathfrak{p}$ *or* $\mathfrak{q} = \mathfrak{p}\mathfrak{p}'$ *depending on whether there is a unique prime* $\mathfrak{p}$ *or two distinct primes* $\mathfrak{p}$ *and* $\mathfrak{p}'$ *of* K' *above* ℓ.

Proof. Since τ_2 and $\tau^{(\ell-1)/2}$ each act by -1 on $G_{\mathfrak{c}}$, $\tau^{(\ell-1)/2}\tau_2$ acts trivially. Writing $e = \frac{1+\tau_2\tau^{(\ell-1)/2}}{2}$, decomposing $1 = e + (1-e) = \frac{1+\tau_2\tau^{(\ell-1)/2}}{2} + \frac{1-\tau_2\tau^{(\ell-1)/2}}{2}$ in $\mathbb{F}_\ell[\Gamma]$, and noting that $G_{\mathfrak{c}}$ is annihilated by

$1-e$, we see that the elements of $G_{\mathfrak{c}}$ are exactly those elements of $\frac{\mathrm{Cl}_{\mathfrak{c}}(K_z)}{\mathrm{Cl}_{\mathfrak{c}}(K_z)^\ell}$ that can be represented by an ideal of the form $\mathfrak{a}\tau_2\tau^{(\ell-1)/2}(\mathfrak{a})$, which we check is of the form $\mathfrak{a}'\mathbb{Z}_{K_z}$ for some ideal $\mathfrak{a}'$ of K'.

As we check, we obtain a well-defined, injective map $G_{\mathfrak{c}} \to \frac{\mathrm{Cl}_{\mathfrak{c}'}(K')}{\mathrm{Cl}_{\mathfrak{c}'}(K')^\ell}[\tau - g]$. To see that it is surjective, observe that any class in $\frac{\mathrm{Cl}_{\mathfrak{c}'}(K')}{\mathrm{Cl}_{\mathfrak{c}'}(K')^\ell}[\tau - g]$ is represented by $I \sim I^{1+\ell}$ for some ideal I of $\mathbb{Z}_{K'}$, and with $\mathfrak{a} = I^{(1+\ell)/2}$ we have $I^{1+\ell}\mathbb{Z}_{K_z} = \mathfrak{a}\tau_2\tau^{(\ell-1)/2}(\mathfrak{a})$.

For (2a), recall that ℓ is totally ramified in K' by Lemma 2.10, so that we must show that $\mathfrak{c} \cap K' = \mathfrak{p}^a$. As ℓ is unramified in $\mathbb{Q}(\sqrt{D})$, we have $e_\ell(K_z/\mathbb{Q}) = \ell - 1$, and if $\mathfrak{P}$ is a prime of K_z above $\mathfrak{p}$ then $v_{\mathfrak{p}}(x) = v_{\mathfrak{P}}(x)$ for any $x \in K'$, hence the result.

For (2b), Lemma 2.10 implies that ℓ has ramification index $\frac{\ell-1}{2}$ in K', and hence that each prime of K' above ℓ has ramification index 2 in K_z/K'. That is, $2v_{\mathfrak{p}}(x) = v_{\mathfrak{P}}(x)$, and the result follows. ∎

We can now obtain the desired bijection for F_ℓ-fields, adapting Proposition 4.1 in [CT14].

Proposition 3.7. *For each Γ-invariant ideal $\mathfrak{c} \mid \mathfrak{b}$, there exists a bijection between the following two sets:*

- *Subgroups of index ℓ of $G_{\mathfrak{c}} = \frac{\mathrm{Cl}_{\mathfrak{c}}(K_z)}{\mathrm{Cl}_{\mathfrak{c}}(K_z)^\ell}[T]$.*
- *Degree ℓ extensions $E/\mathbb{Q}$ (up to isomorphism), whose Galois closure E' has Galois group F_ℓ and contains K', with the conductor $\mathfrak{f}(E'/K')$ dividing $\mathfrak{c}' = \mathfrak{c} \cap K'$, such that $\tau\sigma\tau^{-1} = \sigma^g$ for any generator σ of $\mathrm{Gal}(E'/K')$.*

Remark 3.8. Recall that the element $\tau\sigma\tau^{-1} \in \mathrm{Gal}(E'/K')$ is well defined by Lemma 2.1. Also, note that $\mathfrak{f}(E'/K')$ is Γ-invariant, because E' is fixed by τ_2, courtesy of Proposition 3.6.

Proof. By Proposition 3.6, it suffices to exhibit a bijection between the set of field extensions as above, and subgroups of index ℓ of $G'_{\mathfrak{c}'} := \frac{\mathrm{Cl}_{\mathfrak{c}'}(K')}{\mathrm{Cl}_{\mathfrak{c}'}(K')^\ell}[\tau - g]$, where $\mathfrak{c}' = \mathfrak{c} \cap K$.

Given such a subgroup, we produce a degree-ℓ extension of the desired type. Write $A' := \mathrm{Cl}_{\mathfrak{c}'}(K')/\mathrm{Cl}_{\mathfrak{c}'}(K')^\ell$, and decomposing A' into eigenspaces for the action of τ (as we can, because the order of τ is coprime to ℓ) write $A' \cong G'_{\mathfrak{c}'} \times A''$ where A'' is the sum of the other eigenspaces.

Subgroups $B \subseteq G'_{\mathfrak{c}'}$ of index ℓ are in bijection with subgroups $B' = B \times A'' \subseteq A'$ of index ℓ containing A''. For each B', class field theory gives a unique extension E'/K', cyclic of degree ℓ, of conductor dividing $\mathfrak{c}'$, for which the Artin map induces an isomorphism $G'_{\mathfrak{c}'}/B' \cong \mathrm{Gal}(E'/K')$. Furthermore, E' is Galois over $\mathbb{Q}$ because $G_{\mathfrak{c}'}$ and B' are τ-stable. Each B yields a distinct E', and as the action of $\mathrm{Gal}(K'/\mathbb{Q})$ on the class group matches the conjugation action of $\mathrm{Gal}(K'/\mathbb{Q})$ on $\mathrm{Gal}(E'/K')$ we have $\mathrm{Gal}(E'/\mathbb{Q}) \simeq F_\ell$ with presentation as in the second bullet point. The extension E may be taken to be any of the isomorphic degree ℓ subextensions of E'.

Finally we note that all the steps are reversible, establishing the desired bijection. ∎

Remark 3.9. We now justify the remark made after the statement of our main results concerning the notation * and the primitive roots $\pm g$.

Suppose that $\ell \equiv 1 \pmod 4$, that $\ell \nmid D$, and that τ is a generator of $\mathrm{Gal}(K_z/K)$, so that $\tau\tau_2$ is a generator of $\mathrm{Gal}(K_z/\mathbb{Q}(\sqrt{D\ell^*}))$. Then both K and $\mathbb{Q}(\sqrt{D\ell^*}) = \mathbb{Q}(\sqrt{D\ell})$ have the same mirror field.

Replacing K with $\mathbb{Q}(\sqrt{D\ell})$ is equivalent to replacing τ with $\tau\tau_2$ and thus $T = \{\tau - g, \tau_2 + 1\}$ with $\{\tau\tau_2 - g, \tau_2 + 1\}$, or equivalently, $\{\tau + g, \tau_2 + 1\}$. Thus, if we study D_ℓ-extensions with resolvent $\mathbb{Q}(\sqrt{D\ell})$, where τ is still regarded as a generator of $\mathrm{Gal}(K_z/\mathbb{Q}(\sqrt{D}))$, we obtain the same results with g replaced with $-g$. In particular, in the previous lemma we obtain field extensions E with $\tau\sigma\tau^{-1} = \sigma^{-g}$.

We now show that the set of conductors $\mathfrak{f}(E'/K')$ that can occur in Proposition 3.7 is quite limited.

Proposition 3.10. *The conductors $\mathfrak{f}(E'/K')$ of fields counted in Proposition 3.7 are restricted to the following values:*

- *If $\ell \nmid D$, $v_\ell(\mathfrak{f}(E'/K')) \in \{0, 2\}$.*
- *If $\ell \mid D$ and $\ell \equiv 1 \pmod 4$, $v_\ell(\mathfrak{f}(E'/K')) \in \{0, \frac{\ell+3}{2}\}$.*
- *If $\ell \mid D$ and $\ell \equiv 3 \pmod 4$, $v_\ell(\mathfrak{f}(E'/K')) \in \{0, 2, \frac{\ell+5}{2}\}$.*

Proof. We work with the extensions E''/K_z which correspond to the extensions E'/K' by Proposition 3.6. Unraveling the definition of $G_{\mathfrak{c}}$, we see that the conductor of such an extension can be equal to $(1-\zeta_\ell)^a\mathbb{Z}_{K_z}$ if and only if

$$\frac{1+P^a}{1+P^{a+1}}[T] \neq 0,$$

where $P = (1-\zeta_\ell)\mathbb{Z}_{K_z}$ if this ideal is prime, and P is one of the two primes dividing $(1-\zeta_\ell)\mathbb{Z}_{K_z}$ otherwise. The case $a = 0$ is not excluded in any case listed above; so assuming that $a \geq 1$, we use the inverse Artin-Hasse logarithm and exponential maps, in exactly the same way as on p. 177 of [CDyDO02], to conclude that

$$\frac{P^a}{P^{a+1}}[T] \neq 0. \tag{3.2}$$

Necessary conditions for (3.2) were given in Theorem 1.2 of the first author, Diaz y Diaz, and Olivier's study [CDyDO03] of cyclotomic fields. In all cases P and K_z have the same meaning here and in [CDyDO03].

- If $\ell \nmid D$, then let K have the same meaning as here, and consider the $\tau - g$ eigenspace with $e(\mathfrak{p}) = 1$. Then Theorem 1.2 implies that $a \equiv 2 \pmod{\ell-1}$.
- If $\ell \mid D$ and $D \equiv 1 \pmod 4$, let K of [CDyDO03] be $\mathbb{Q}(\sqrt{D\ell})$, so that the T-eigenspace lies within the $\tau - g^{(\ell+1)/2}$ eigenspace. Then Theorem 1.2 implies that $a \equiv \frac{\ell+3}{2} \pmod{\ell-1}$.
- If $\ell \mid D$ and $D \equiv 3 \pmod 4$, then again K has the same meaning in [CDyDO03] as here; now $e(\mathfrak{p}) = 2$, so that $a \equiv 2 \pmod{\frac{\ell-1}{2}}$.

So, given that $a \leq \ell - 1$, we obtain respectively in these three cases for $\mathfrak{f}(E''/K_z)$ that $a \in \{0, 2\}$, $a \in \{0, \frac{\ell+3}{2}\}$, and $a \in \{0, 2, \frac{\ell+3}{2}\}$. By Proposition 3.6 the corresponding values for $\mathfrak{f}(E''/K_z)$ are a, a, and $2\lceil\frac{a}{2}\rceil$, so $a \in \{0, 2\}$, $a \in \{0, \frac{\ell+3}{2}\}$, and $a \in \{0, 2, \frac{\ell+5}{2}\}$ respectively. ∎

4. Proofs of the Main Results

Proof of Theorem 1.2. Let $K = \mathbb{Q}(\sqrt{D})$ with $D < 0$. The key to the proof is the identity $|G_{\mathfrak{b}}| = |\mathrm{Cl}(K)/\mathrm{Cl}(K)^\ell|$ of Proposition 3.5. By Lemma 2.8, $\frac{1}{\ell-1}(|G_{\mathfrak{b}}|-1)$ equals the number of D_ℓ extensions with discriminant $(-1)^{\frac{\ell-1}{2}}D^{\frac{\ell-1}{2}}$. Simultaneously, Propositions 3.6 and 3.7 imply that $\frac{1}{\ell-1}(|G_{\mathfrak{b}}|-1)$ is the number of F_ℓ extensions whose Galois closure E' contains the mirror field K', with $\mathfrak{f}(E'/K') \mid \mathfrak{b} \cap K$, and with $\tau\sigma\tau^{-1} = \sigma^g$ as described there. Theorem 2.12 implies that the Galois closure of each F_ℓ-field described in the theorem must contain K', so that it remains only to prove that the condition $\mathfrak{f}(E'/K') \mid \mathfrak{b} \cap K$ coincides with the discriminant conditions on the F_ℓ-fields counted in the theorem.

First assume that $\ell \equiv 1 \pmod 4$ or $\ell \nmid D$ (or both). Then Lemma 2.10 implies that $\mathrm{Disc}(K') = \ell^{\ell-2}(-D)^{\frac{\ell-1}{2}}$ or $\mathrm{Disc}(K') = \ell^{\ell-2}(-D/\ell)^{\frac{\ell-1}{2}}$, if $\ell \nmid D$ or $\ell \mid D$, respectively. Thus, we have

$$v_\ell(\mathrm{Disc}(E')) = \ell(\ell-2) + (\ell-1)\mathfrak{f}_{\mathfrak{p}}(E'/K')\,, \tag{4.1}$$

where $\mathfrak{p}$ is the unique (totally ramified) ideal of K' above ℓ. Writing $k = \mathfrak{f}_{\mathfrak{p}}(E'/K')$, Propositions 3.6, 3.7, and 3.10 imply that the fields counted are precisely those with $k \in \{0, 2\}$ or $k \in \{0, \frac{\ell+3}{2}\}$ for $\ell \nmid D$ and $\ell \mid D$ respectively, so that the Brauer relation (2.7) implies that $v_\ell(\mathrm{Disc}(E)) \in \{\ell - 2 + k\}$ with k as above.

If instead $\ell \equiv 3 \pmod 4$ and $\ell \mid D$, then we have $\mathrm{Disc}(K') = \ell^{\ell-3}(-D/\ell)^{\frac{\ell-1}{2}}$ and

$$v_\ell(\mathrm{Disc}(E')) \in \{(\ell-3)\ell + (\ell-1)k : k \in \{0, 2, (\ell+5)/2\}\}, \tag{4.2}$$

with $k \neq 2$ because the ℓ-adic valuation of the discriminant of a degree ℓ field cannot be $\ell - 1$.

For each prime $q \neq \ell$ dividing D, E'/K' is unramified at primes over q, so that by (2.7) we have $v_q(\mathrm{Disc}(E)) = v_q(\mathrm{Disc}(K'))$. Also, E must be totally real, because K' is and $[E' : K']$ is odd. Put together, in all cases this shows that $\mathrm{Disc}(E)$ is equal to $D^{\frac{\ell-1}{2}}$ times a power of ℓ as prescribed in Theorem 1.2, finishing the proof. ∎

Proof of Theorem 1.3. The proof is essentially identical, now using the $D > 0$ case of Proposition 3.5, applying the identity $\ell \cdot \frac{\ell^a-1}{\ell-1} + 1 = \frac{\ell^{a+1}-1}{\ell-1}$, and obtaining the signature of E by (2.7). ∎

5. Numerical testing

Our work began with $\ell = 5$, by inspecting the Jones-Roberts database of number fields [JR13] and finding patterns which called for explanation. However, for $\ell > 5$, this database does not contain enough fields for a reasonable test, and does not include the Galois conditions featuring in our theorems.

We therefore wrote a program using `Pari/GP` [PAR14] to compute the relevant number fields, for which source code is available from the third author's website[1]. A few comments on this program:

Thanks to the relation $\mathrm{Disc}(E) = \mathrm{Disc}(F)\mathcal{N}(\mathfrak{f}(E'/F))$ given after (2.6), to enumerate F_ℓ fields (possibly with certain conditions, including discriminant and/or Galois restrictions), it is enough to enumerate suitable $C_{\ell-1}$ fields F (which is very easy), and for each such field to enumerate suitable conductors $\mathfrak{f}$ of C_ℓ-extensions E'/F such that $E'/\mathbb{Q}$ is Galois. Luckily, these Galois conditions imply that these suitable conductors are very restricted, since they must be of the shape $\mathfrak{f} = n\mathfrak{a}$, where n is an ordinary integer and $\mathfrak{a}$ is an ideal of F divisible only by prime ideals of F which are above ramified primes of $\mathbb{Q}$, and in addition which must be Galois stable.

For each conductor $\mathfrak{f}$ of this form, we compute the corresponding ray class group, and if it has cardinality divisible by ℓ, we compute the corresponding abelian extension, and check which subfields of degree ℓ of that extension satisfy our conditions.

Note that for our purposes, we only *count* the F_ℓ-extensions that satisfy our conditions. Our program can also compute them explicitly thanks to the key `Pari/GP` program `rnfkummer`, for which the algorithm is described in detail in Chapter 5 of the first author's book [Coh00].

Our numerical testing was moderately extensive for $\ell = 5$ and $\ell = 7$, and rather limited for $\ell = 11$ and $\ell = 13$, as the complexity of our algorithms grows rapidly with ℓ. We verified our results and found F_ℓ-fields with all the powers of ℓ given in our main theorems, with the exception of 13^4. The computational complexity of our algorithm severely limited the amount of testing we could conduct with $\ell = 13$; we speculate that the power of ℓ not found is uncommon but does exist.

References

[Bha04] Manjul Bhargava. Higher composition laws. III. The parametrization of quartic rings. *Ann. of Math. (2)*, 159(3):1329–1360, 2004.

[1] `http://www.math.sc.edu/~thornef/`

[Bha05] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2):1031–1063, 2005.

[CDyDO02] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. On the density of discriminants of cyclic extensions of prime degree. *J. Reine Angew. Math.*, 550:169–209, 2002.

[CDyDO03] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. Cyclotomic extensions of number fields. *Indag. Math. (N.S.)*, 14(2):183–196, 2003.

[CDyDO06] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. Counting discriminants of number fields. *J. Théor. Nombres Bordeaux*, 18(3):573–593, 2006.

[CM11] Henri Cohen and Anna Morra. Counting cubic extensions with given quadratic resolvent. *J. Algebra*, 325:461–478, 2011.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Coh04] Henri Cohen. Counting A_4 and S_4 number fields with given resolvent cubic. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 159–168. Amer. Math. Soc., Providence, RI, 2004.

[CT13a] H. Cohen and F. Thorne. Dirichlet series associated to quartic fields with given resolvent. *ArXiv e-prints*, February 2013.

[CT13b] H. Cohen and F. Thorne. On D_ℓ-extensions of odd prime degree ℓ. *In preparation (draft available upon request)*, 2013.

[CT14] Henri Cohen and Frank Thorne. Dirichlet series associated to cubic fields with given quadratic resolvent. *Michigan Math. J.*, 63(2):253–273, 2014.

[DDT97] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997.

[FT93] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[Gre89] Ralph Greenberg. Iwasawa theory for p-adic representations. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 97–137. Academic Press, Boston, MA, 1989.

[JR13] J. Jones and D. Roberts. Number fields. 2013. `http://hobbes.la.asu.edu/NFDB/`.

[KMTB13] N. Kaplan, J. Marcinek, and R. Takloo-Bighash. Counting subrings of $\mathbb{Z}^n$ of finite index. *ArXiv e-prints*, 2013.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Nak96] Jin Nakagawa. Orders of a quartic field. *Mem. Amer. Math. Soc.*, 122(583):viii+75, 1996.

[Nak98] Jin Nakagawa. On the relations among the class numbers of binary cubic forms. *Invent. Math.*, 134(1):101–138, 1998.

[NO] Jin Nakagawa and Yasuo Ohno. Unpublished preprint.

[Ohn97] Yasuo Ohno. A conjecture on coincidence among the zeta functions associated with the space of binary cubic forms. *Amer. J. Math.*, 119(5):1083–1094, 1997.

[PAR14] PARI Group, Bordeaux. *PARI/GP, version* `2.6.2` *(tested using version* `2.5.1`*)*, 2014. Available from `http://pari.math.u-bordeaux.fr/`.

[Poi67] Georges Poitou. *Cohomologie galoisienne des modules finis*, volume 13 of *Séminaire de l'Institut de Mathématiques de Lille*. Dunod, 1967.

[Sch32] Arnold Scholz. Über die Beziehung der Klassenzahlen quadratischer Körper zueinander. *Journal für die reine und angewandte Mathematik*, 166:201–203, 1932.

[Ser67] J.-P. Serre. Local class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 128–161. Thompson, Washington, D.C., 1967.

[Tat63] John Tate. Duality theorems in Galois cohomology over number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 288–295. Inst. Mittag-Leffler, Djursholm, 1963.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Université de Bordeaux, Institut de Mathématiques, U.M.R. 5251 du C.N.R.S, 351 Cours de la Libération, 33405 TALENCE Cedex, FRANCE
E-mail address: Henri.Cohen@math.u-bordeaux1.fr

Department of Statistics, Stanford University, 390 Serra Mall, Stanford, CA 94305, USA
E-mail address: simonr@stanford.edu

Department of Mathematics, University of South Carolina, 1523 Greene Street, Columbia, SC 29208, USA
E-mail address: thorne@math.sc.edu